Service Organization Controls (SOC) 3
for Security, Availability, Confidentiality, and Processing Integrity

Independent Practitioner's Trust Services Report

For the Period December 1, 2018 to November 30, 2019

Independent SOC 3 Report for Security, Availability, Confidentiality, and Processing Integrity Trust Services Criteria for LegalShield.

TABLE OF CONTENTS

Section 1	Independent Practitioner's Trust Services Report	1
Section 2	Assertion of LegalShield Management	3
Section 3	Attachment A: Description of LegalShield's System	5
Section 4	Attachment B: Principal Service Commitments and System Requirements	21

SECTION ONE: INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To: LegalShield

Scope

We have examined LegalShield's accompanying assertion titled "Assertion of LegalShield Management" (Assertion) that the controls within LegalShield's system (System) were effective throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that LegalShield's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

LegalShield is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that LegalShield's service commitments and system requirements were achieved. LegalShield has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LegalShield is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve LegalShield's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve LegalShield's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within LegalShield's system were effective throughout the period December 1, 2018 to November 30, 2019 to provide reasonable assurance that LegalShield's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material aspects.

CyberGuard Compliance, LLP
January 13, 2020
Orange, California

SECTION TWO: ASSERTION OF LEGALSHIELD MANAGEMENT

January 13, 2020

Scope

We are responsible for designing, implementing, operating, and maintaining effective controls within LegalShield's system (System) throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that LegalShield's service commitments and system requirements relevant to security, availability, confidentiality and processing integrity were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that LegalShield's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and processing integrity (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, *Trust Services Criteria).* LegalShield's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

LegalShield uses various subservice organizations to supplement their services. The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at LegalShield, to achieve LegalShield's service commitments and system requirements based on the applicable trust services criteria. The description presents LegalShield's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of LegalShield's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary are necessary to achieve LegalShield's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2018 to November 30, 2019, to provide reasonable assurance that LegalShield's service commitments and system requirements were achieved based on the applicable trust services criteria.

LegalShield

SECTION THREE:

ATTACHMENT A: DESCRIPTION OF LEGALSHIELD'S SYSTEM

1 Overview of LegalShield's Operations

Our goal at LegalShield is to revolutionize the way legal services are delivered in North America by providing access to quality law firms for individuals and families. Everyone deserves legal protection, and with LegalShield everyone can access it.

Founded in 1972 in Ada, Oklahoma, LegalShield is a leading provider of legal plans and identity theft solutions to families and small businesses across the U.S. and Canada. LegalShield markets its products through two main channels: Business-to-Business and Networking. Independent benefit brokers provide the products to corporate employees through payroll deduction. More than 34,000 companies offer LegalShield plans to their employees. With 1.75 million families enrolled, LegalShield's legal plans currently protect 4.4 million people in 50 U.S. states and four Canadian provinces. LegalShield is the only national legal safeguard to provide its participants with access to quality legal services from an accomplished law firm in their state or province for legal advice and assistance no matter how trivial or serious the issue. For a low monthly fee, LegalShield participants get access to qualified attorneys who are experts in the areas of law that most impact families and small businesses. LegalShield provides dedicated provider law firms throughout the U.S. and Canada enabling participants to feel as though they have their own personal law firm to call for help without having to worry about high hourly rates. LegalShield identity theft plans currently cover 1.7 million people with nearly 10,000 identities restored. Our identity theft plans provide more than just credit monitoring – we also provide consultation on any identity theft issue and complete identity restoration in the event an identity is stolen. We field more than two million calls each year. With over 700 LegalShield employees dedicated to serving our groups and their employees, our promise is to provide outstanding legal and identity theft services at an affordable price.

Our corporate operation is headquartered in Ada, Oklahoma, with offices in Oklahoma City, OK and two remote call centers located in Duncan, OK and Antlers, OK. The headquarters facility consists of a 177,000 square foot, state-of-the-art complex that houses all operational departments supporting membership application entry and related processing. The facility houses call centers handling customer service for members and associates, including staff responsible for commission payments, receipt of membership fees, general ledger accounting, human resources, internal audit and a department that manages and monitors provider law firm relationships. The IT data centers are located in the headquarters facility and in Oklahoma City, Oklahoma. LegalShield uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

2 Overview of the System and Applications

System Overview

The System is comprised of the following components:

- ***Network and Infrastructure***: The physical and hardware components of a system (facilities, equipment, and networks);
- ***Software***: The programs and operating software of a system (systems, applications, and utilities);
- ***Data***: The information used and supported by a system (transaction streams, files, databases, and tables);
- ***People***: The personnel involved in the operation and use of a system (developers, operators, users, and managers); and
- ***Procedures***: The automated and manual procedures involved in the operation of a system.

Network and Infrastructure

The IT network operates on a Microsoft Windows-based platform, using IBM client access to connect to their proprietary Customer Relationship Management software on the IBM System i. The IBM System i also houses a DB2 database that is the primary data store for the business. For security and redundancy purposes, multiple servers are used for various service delivery functions and applications.

LegalShield's infrastructure consists of two IBM Power Systems, one at each data center location. These servers support the core business applications and databases with real-time replication between the systems. In addition, there are a number of cloud services and virtual machines supporting various functions. Employees use desktop PCs, laptops running Windows and macOS productivity applications, and as well as Power Systems terminal emulation on a Windows server network.

- One Primary Database server and one Backup Database server
- Multiple Web servers
- Multiple Domain Control servers
- Security servers are deployed for intrusion detection, centralized logging, application scanning, device scanning and file integrity monitoring
- Cisco, F5, and Fortinet Firewalls deployed inline
- NICE inContact Cloud-Based Contact Center Solution

Physical Security at Corporate Headquarters
Security guards and video cameras are present throughout the building grounds and within the building. The buildings and grounds are monitored 24 x 7. The first layer of physical security is the gate at the entrance to the property. Visitors are required to stop and check with the security guard at the main gate before gaining access to the parking area.

The second layer of physical security are the proximity card key readers, software and badges that control physical access to the buildings and all secured areas within the building. Off-hour access to the gate at the entrance to the property is controlled by card key access.

The third layer of physical security is the restriction of physical access to the information centers to only those staff members required to have access to complete their job functions. All other staff members and vendors are required to sign in and must be escorted for the duration of their visit. Hardware running corporate applications is housed in a secured area with appropriate controls and monitoring. Restricting physical access ensures that computing assets (servers, network, information, etc.) are not exposed to unwarranted risks.

Logical Security
Security software and devices are used to protect against unauthorized access, destruction, disclosure or modification of information and applications programs. Logical access controls are layered and govern access to the network, servers, applications and information. Logical access to the network, servers, applications and information is restricted to only those staff members required to have access to complete their job functions.

All employees and contractors are required to log in to the internal network and authenticate, which is the first layer of logical security. Once network access has been authenticated, an internal user may log in to servers or applications, which requires additional authentication and is the second layer of logical security. Access privileges for users are established via a standard authorized access request process and granted in accordance with job-related duties. LegalShield's Content Management System for corporate websites can be accessed directly from the web for authorized employees and contractors.

Systems are configured to maximize the enforcement of security. LegalShield uses proper user ID and password procedures to ensure security, and all users must have unique user IDs to gain access to systems.

Data Protection
LegalShield has an information classification system for all information under LegalShield's control. Information classified as Confidential or Restricted is stored in a physically secure location.

All Confidential information is encrypted when transmitted across public networks. Credit card information is transmitted to a third-party credit card processing company who clears the transactions and processes the payments. The credit card processing company has security practices in place to protect this information and is audited independently. When documents containing Confidential or Restricted information are disposed of, the documents are placed inside a locked shred bin or shredded immediately.

LegalShield's electronic billing department verifies encryption methods that meet Company requirements are used when sensitive information, such as electronic deposits and member information, is transmitted or received.

Incident Detection, Response and Reporting

A variety of resources is employed to record and analyze system activity for the express purpose of identifying unusual conditions or suspect activity. Exceptions are logged and investigated. Incident detection procedures require that a suspected or actual incident be escalated immediately. Management is committed to following LegalShield's Incident Response Plan and all applicable local, state and federal law.

Environmental Protections

Computer operations and servers are protected by the following safeguards and environmental control systems:

a. Smoke detectors
b. Fire alarm system
c. Raised floors
d. Climate conditioning
e. Emergency power-off
f. UPS including battery backup and diesel generator power
g. Automatic fire suppression system
h. Hand-held fire extinguishers
i. Water detectors
j. Temperature and humidity control devices
k. Emergency lighting

Proactive Assessments
Regular internal and external vulnerability assessments are performed to proactively manage potential risks to network and server security. LegalShield hires security experts to conduct annual internal and external vulnerability assessments. Additionally, LegalShield's in-house staff conducts quarterly internal and external vulnerability assessments. The assessment findings provide confirmation of working security practices and identify opportunities for improvement. Any findings or recommendations are discussed, and appropriate corrective action is taken to address any real or suspected vulnerabilities. This is a continual improvement process to LegalShield's overall infrastructure and security posture.

Internal controls are required by executive management to confirm LegalShield's strong security measures. Best practices have been implemented for all security measures where possible. Third-party auditors and controls experts are contracted with to test and verify that internal controls for business applications and information technology are designed and operating effectively. This testing is further confirmation that effective security measures are in place and that your information is protected.

On a regular basis, systems and information users are reviewed to ensure access is restricted based upon job duties. LegalShield uses the least-privilege concept for providing access to information resources. Users have only the access necessary to perform their job duties. Department managers direct appropriate changes to user access for their employees. When changes are made to user access, the department manager is required to confirm the changes were implemented.

Software

The business develops critical applications in-house, which are supported by internal staff and contractors. These applications include member application entry, commissions, cash receipts, credit card processing, electronic bank draft, premium billing, claims, customer relationship management, web sites, mobile, group sites, and intake management administration for provider attorneys. Critical business data is hosted on premise.

People

Bios of key LegalShield Personal

Jeff Bell , Chief Executive Officer and Board of Directors, was named Chief Executive Officer of LegalShield in July 2014. Since his arrival, LegalShield has grown to over 1.7 million members, protecting and empowering over 4 million lives. Previously, Mr. Bell was Corporate Vice President, Global Marketing, Xbox, for Microsoft Inc. from 2006 to 2009. He spent 12 years at Ford Motor Company, including serving as Managing Director of Ford Spain, and 5 years at Chrysler as the Vice President and General Manager of Chrysler and Jeep Divisions. Jeff earned the 2008 Cannes Grand Prix Winner for the Halo 3 Integrated Marketing campaign. He was named AdAge "2007 Entertainment Marketer of the Year" for Gears of

War, and AdAge “2005 Interactive Marketer of the Year” at Chrysler. He has served as Trustee of his alma mater, Kenyon College, and on the Board of the National Multiple Sclerosis Society. Bell graduated from Kenyon College Magna Cum Laude, Phi Beta Kappa and was honored as an Academic All-American in football. He holds Master’s degrees from Johns Hopkins and Wharton.

Kathy Pinson, EVP, Chief Operations Officer, currently serves as LegalShield's Chief Operating Officer, working with and supporting all Vice Presidents of LegalShield, coordinating all administrative functions within the home office and field operations. With the company since 1979, Kathy has served with distinction in a number of roles, including Controller, Board Member, Secretary/Treasurer, Vice President of Marketing Administration and Executive Vice President of Operations. Ms. Pinson is a Certified Public Accountant and served more than 20 years managing the regulatory compliance division of the company.

Steve Williamson, EVP, Chief Financial Officer, has been with LegalShield for over 12 years. Prior to joining the company, he served as the Chief Financial Officer for Peripheral Enhancements, Inc. from April 1997 to March 2000. Steve served as Director in Charge of Banking Practice for Horne & Company, a public accounting firm, from November 1983 to April 1997. After graduating from East Central University in 1982, he began his career with the international accounting firm KPMG. Since 2000, Steve has served as LegalShield's Chief Financial Officer. He is a Certified Public Accountant (CPA) and is a past board member and banking committee chair of the Oklahoma Society of CPAs.

Darnell Self, EVP of Network & Business Development, After earning a degree in public relations at Bowie State University, Darnell Self joined LegalShield in 1998. He has shared his vast experience in team building, personal development, and entrepreneurship since day one. These experiences allowed Mr. Self to orchestrate a duplicable system, garnering recognition in numerous business publications and the esteemed title of Entrepreneur of the Year by the National Black Chamber of Commerce. He is also a mentor to thousands of thriving entrepreneurs and has been asked to share his expertise with business students on several university platforms. Coming from humble beginnings, Mr. Self has devoted his time and efforts to give people, no matter the circumstance, an opportunity to actualize their own success. This level of commitment has resulted in dozens of LegalShield Ring Earners and over a dozen Millionaire Club Members. Mr. Self and his colleague Michael Humes also collaborated to create Fertile Ground – an organization designed to allow others to experience the power of giving.

Alan Madden, EVP, Chief People Officer, joined LegalShield in 2018 and was named Senior Vice President, Chief People Officer to oversee all aspects of our Human Resources, Workplace Policies, and Facilities. Alan is an accomplished global human resources executive with over 23 years of HR experience in legal services, manufacturing, oil and gas, aerospace, automotive, hospitality, and retail industries. Alan has earned a solid reputation as a results-

oriented, “shirt-sleeves up” HR professional with a clear understanding of the operational and people issues facing today’s business leaders.

Keri C. Norris, EVP, Legal & Regulatory Affairs and General Counsel, joined LegalShield as its first General Counsel in 2003. She oversees the company's legal affairs, including litigation, corporate legal matters, and regulatory and governmental matters. She also serves as an advisor to the company's executive management team. Prior to joining LegalShield, she was an associate attorney at Crowe & Dunlevy in Oklahoma City and at Hunton & Williams in Raleigh, North Carolina, where she specialized in commercial litigation, intellectual property litigation, and creditor's rights and bankruptcy. Ms. Norris is a member of the Association of Corporate Counsel of America, American Bar Association, the Oklahoma and North Carolina Bar Associations and the Pontotoc County Bar Association. She serves on the American Bar Association Standing Committee on Group & Prepaid Legal Services and the Group Legal Services Association. She earned a B.A. (English) and a J.D., both summa cum laude, from Oklahoma City University.

Jack Goldenberg, EVP, Chief Technology Officer, joined LegalShield in January 2015 to establish and lead the company's technical vision and development, including strategy for technology platforms and partnerships. In his previous career, he served Meredith Corporation as Senior Vice President and Chief Technology Officer for the National Media Group. In this role, Jack managed the delivery of Meredith Digital Tablet editions for all of the Meredith Magazine brands, including interactive editions for Better Homes and Gardens, Parents, Fitness, and Family Fun. Prior to Meredith, Jack served as Chief Technology Officer for Enterprise Media Group at Dow Jones and Company. He was responsible for delivering the innovative Dow Jones Investment Banker and Dow Jones Adviser digital products. His background also includes serving as the Senior Vice President, Content Technology for Thomson Reuters/Thomson Financial. Under his leadership, Thomson Reuters was able to implement new technology to streamline the data acquisition and delivery process resulting in faster and more reliable delivery to the customer. Mr. Goldenberg holds a bachelor's degree in Professional Science from C.W. Post University. He also served as a Board Member for the Des Moines Playhouse, a nonprofit organization, from 2011 through 2014.

Glen Peterson, President of LegalShield Business Solutions, is President of LegalShield’s Business Solutions division, responsible for business development, strategy and sales growth for LegalShield’s affinity, broker, voluntary benefits, national accounts and small business divisions. He has 25 years of experience in the benefit space and is an industry expert in the worksite voluntary benefits arena. Glenn previously served as SVP of LegalShield’s Broker and Partnership Sales and was a VP at Metlife for nearly 10 years. He has managed and led many successful voluntary benefit sales organizations making him well-versed in voluntary benefits.

Don Thompson, President of Network Division, joined LegalShield in 1996 as an Independent Associate. During his career as an associate, Mr. Thompson has earned many top achievements, business builder, and production awards. He has served in many field

leadership positions including Regional Vice President of Florida, Business Vice President of Florida, Ohio, and Michigan, and most recently, Sr. Network Vice President of 26 states and 2 provinces of Canada. Mr. Thompson has mentored and trained thousands of associates by teaching the fundamentals of leadership and personal development. Don Thompson was named President of the Network Division in December 2018. He is a graduate of John Carroll University, Boler School of Business, with a degree in Business Administration.

Scott Grissom, Chief Product Officer, joined LegalShield in June 2018 and was named Chief Product Officer in December 2018. Scott's most recent professional experience was as Chief Financial Officer of Ferrari North America, which was preceded by 25+ years in Corporate Finance at various incarnations of Fiat Chrysler Automobiles (FCA). While at FCA, Scott specialized in supporting various Sales and Marketing areas including business planning, brand development, media planning, advertising production, pricing, and automotive financial services. Scott has an BS in Finance from Ohio State University, and an MBA from Columbia University.

Martine Girotto, President of LegalShield Canada, with over 17 years' experience in various roles and capacities, Martine brings a wealth of contribution and knowledge within the Direct Sales Industry. Prior to joining LegalShield, Martine served as General Manager of Canada at Jeunesse Global for 3 years, where she was responsible for the market strategy, sales, leadership development and marketing efforts in Canada. As well, with more than 10 years as Director of Sales at Mary Kay Cosmetics, Canada, Martine has developed a passion for the industry and her strong work ethics paired with her ability to balance strategy and tactics have allowed her to gain influence with field and corporate leaders alike. Her degree in psychology and her love for helping others, makes her a great asset for the Canadian market.

Todd Barrs, VP of Direct to Consumer, joined LegalShield in 2018. Prior to joining the company, he served as VP of Ecommerce at multiple technology start-ups where he led numerous successful digital transformation initiatives. Todd has developed and implemented digital and eCommerce programs for a wide range of B2C and B2B organizations in the enterprise SaaS, software security, telecom, online education, apparel and CPG industries. He is a nationally recognized speaker on the topics of digital strategy, web analytics and website testing. Todd holds an MBA from The George Washington University and a BS in Mechanical Engineering from Colorado State University.

Data

All information is stored on LegalShield servers located in the United States. Information is treated as an asset that must be protected against loss and unauthorized access. Procedural and technical safeguards are in place to protect personal information against loss or theft as well as unauthorized access and disclosure. Security technologies are utilized to protect information from unauthorized access inside and outside of LegalShield.

Extended Validation Secure Socket Layer certificates are in use when personal information is uploaded or viewed on the LegalShield website. Each associate and member have a unique username and password that must be entered every time a user logs on to the website. Firewalls and layered security technologies prevent interference or access from outside intruders. The website is hosted on servers located in a secure data center.

LegalShield collects non-public personal information from the following sources:

- Information that is received from applications or other forms such as name, address, social security number, and payment instructions
- Information that is provided during visits to the LegalShield web site or calls to customer service representatives
- Information about your transactions with LegalShield, its affiliates or others.

LegalShield does not disclose non-public personal information about customers or former customers to non-affiliated entities except as described below and otherwise permitted by law. LegalShield may disclose information collected, as described above, to Provider Law Firms and companies that assist in the servicing or administration of the product that has been requested and authorized.

When information is shared with companies that perform services on behalf of LegalShield, LegalShield protects against the subsequent disclosure of that information with a confidentiality agreement.

In no event does LegalShield disclose personal information to companies that will use that information to contact you about their own products or services.

Boundaries of the System

The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. The boundaries of LegalShield's system include applications and infrastructure that directly support the services provided to LegalShield's members and associates. Applications, databases, and infrastructure that indirectly support the services provided to LegalShield's clients are not included within the boundaries of LegalShield's system.

Procedures

New Member and Group Accounts
LegalShield has a series of procedures to setup new member and group accounts that use its legal services and identity theft products, including:

- Setup new member accounts based on the type of plan purchased

- Setup secure data transfer for group accounts
- Setup individual authorized member users and group accounts for their web platform

Once new member accounts have been established within the system, the following activities occur to ensure services are performed accurately, completely and timely:

- Member Services Representatives answer calls from members about services
- Quality assurance reviews Member Services calls
- Provider Services Representatives help members with complaints and referrals

The system has statistical information management tools for recording all services during the circle of the process workflow, including the services volume, services turnaround time. Additionally, the system has built-in audit trails for tracking all information alteration or correction activities. All system informational changes performed are recorded by the system with a time stamp.

Secure Access to Information Assets
LegalShield communicates the established security policies, user rights and responsibilities, and restrictions to the employees of the company. Management performs annual reviews of user access profiles and ensures that the appropriate people are assigned to those profiles. The number of employees that have administrator rights to hardware or applications is restricted. Logs are reviewed to ensure that the use of administrative rights is appropriate. The setup, change, or elimination of user rights follows established procedures.

LegalShield performs intrusion detection testing. All firewall and networking hardware is reviewed for proper configuration and proper software levels. Firewall and network logs are reviewed for security events. Potential security or intrusion events are monitored on the network and servers. Remote access is restricted, controlled, and required to have security authentication before allowing access. Data that is sensitive is transmitted in a protected format, such as through a VPN or with appropriate levels of encryption.

Develop, Acquire, Implement, and Maintain Software
LegalShield has established procedures for the systems development lifecycle, project management, and change management to govern applications development and maintenance. These procedures are designed to facilitate an orderly development process with appropriate review, testing, and audit trails, ensuring segregation of duties between programmers and the production environment.

LegalShield reviews system event and activity logs. Processes are used to ensure system software is upgraded to assist in preventing security breaches. Software that is LegalShield to systems is tested before implementation. A process exists to purchase software and track software licensing compliance after its purchase.

Scope

The scope of the review is limited to LegalShield's Legal Services System.

Trust Service Criteria

The five Trust Service Criteria are defined as follows:

- **Security**: The system is protected against unauthorized access (both physical and logical).
- **Availability**: The system is available for operation and use as committed or agreed.
- **Processing Integrity**: System processing is complete, accurate, timely, and authorized.
- **Confidentiality**: Information designated as confidential is protected as committed or agreed.
- **Privacy**: Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA).

This report encompasses the Security, Availability, Processing Integrity and Confidentiality Trust Service Criteria and does not include Privacy.

Control Environment

Key facets of the Company's control environment relating to processing and staffing for all processes performed by the Company are summarized below. These areas include:

- Integrity and Ethical Values
- Commitment to Competence
- Management's Philosophy and Operating Style
- Human Resources Policies and Practices
- Organizational Structure and Assignment of Authority and Responsibility

Integrity and Ethical Values

LegalShield encourages a fair and open atmosphere to govern professional conduct. LegalShield sets out to provide a professional climate and physical working environment that supports all staff in their daily duties and tasks.

All LegalShield employees adhere to a strict code of ethics with an assurance of confidentiality. Employees receive annual training on the use of confidential information. The Confidentiality Agreement governs the usage of the systems and the treatment of confidential information within the LegalShield environment.

Commitment to Competence

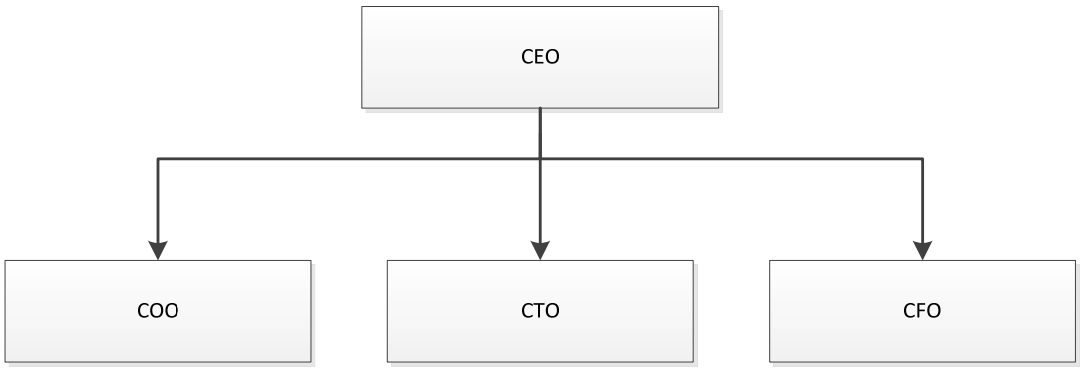
LegalShield has an established IT staff training process. LegalShield has written job descriptions and a career path matrix for all IT positions within the department.

Management's Philosophy and Operating Style

LegalShield has established an IT governance process, which includes an Office of Chief Executives (OCE), to review, approve and prioritize IT plans. This process has been communicated to LegalShield management, and key members of the management team participate in the governance process.

LegalShield has established an IT vendor management process and a centralized IT contracts archive. Additionally, a risk assessment process is in place at both an enterprise level and at a project level. The enterprise-level process includes a quarterly review and the Systems Development Lifecycle Procedure provides for project-level risk assessments.

Organizational Structure and Assignment of Authority and Responsibility



Human Resources Policies and Practices

LegalShield is committed to equal opportunity of employment. Employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. LegalShield endorses a work environment free from discrimination, harassment, and sexual harassment.

Executive management, supervisors or special appointed employees in concert with Human Resources personnel within LegalShield are responsible for the screening and selection of potential employee candidates, and for overall personnel hiring. During the hiring process, candidates are assessed through a series of interviews and/or technical tests to determine if they have the appropriate qualifications and skills to meet the needs of vacant positions. Once final candidates have been identified, job offers are made, contingent upon successful background checks.

An Employee Handbook is distributed to all new employees. The handbook includes professional and work standards, policies and procedures, benefits, and administrative procedures. All employees are required to sign an acknowledgement of Handbook receipt, indicating their understanding of, and agreement to comply with the standards, policies and procedures.

LegalShield has implemented policies and standard operating procedures that contain formal and documented policies relevant to human resources, IT administration, and business operations defining responsibilities, standards, and expectations from their employees.

HR policies and procedures are documented in the Employee Handbook and cover management practices as they relate to the following:

- Equal opportunity employment
- Employment status
- Benefits
- Safety and security
- Quality performance
- Attendance and compensation
- Protection of LegalShield interests
- Employee code of ethics
- Harassment policy
- Confidentiality

In addition, the Information Technology (IT) department maintains policies for the following:

- Change control
- Problem or issue management
- Remote access
- Password policy
- Data sensitivity
- Data handling and disposal

LegalShield requires that all new employees undergo general company training upon being hired. All departments are responsible for providing additional and specific training on as needed bases or as required through performance reviews. Web developers must also undergo secure coding training.

Risk Assessment

"Risk" is defined as the possibility that an event will occur and adversely affect the achievement of objectives. LegalShield recognizes the importance of risk management and properly managing risk that affects our ability to provide high-quality, cost effective services

to our members, associates and provider law firms. The Executive VP of Operations and Chief Financial Officer identify and analyze financial risks in order to develop and manage appropriate responses to risks within acceptable levels and with great focus on fraud and material misstatement. The Chief Technology Officer and Chief Information Security Officer oversee the assessment of risk with respect to the IT processing environment and related application systems and services provided to users of the company's application systems.

Monitoring

LegalShield management and supervisory personnel monitor internal control performance quality as a routine part of their activities. To assist them in this monitoring, LegalShield has implemented a series of management reports that measure various aspects of internal operations to 1) determine if objectives are achieved, 2) identify risks that develop, and 3) implement appropriate measures to address those risks. All exceptions to normal or scheduled processing related to hardware, software, or procedural problems are logged, reported, and resolved daily. LegalShield has adopted a proactive approach in monitoring applications security, availability, processing integrity and confidentiality to ensure that issues or risks are addressed.

Monitoring of Subservice Organizations

LegalShield utilizes Vantiv and Vindicia as their credit card payment processor. Management of LegalShield receives and reviews the SOC 2 reports of Vantiv and Vindicia on an annual basis, including the Complementary Subservice Organization Controls (CSOC) included within the SOC 2 reports. In addition, through its daily operational activities, management of LegalShield monitors the services performed by Vantiv and Vindicia to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

Information and Communication

Communication

LegalShield has implemented various methods of communication to determine all employees understand their individual roles and responsibilities or transaction processing and controls, and to determine that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees. Departmental managers and supervisors are responsible for providing specific departmental training as required to fulfill specific tasks. Managers also hold periodic staff meetings as appropriate. LegalShield has established policies and procedures that are formally documented and clearly communicated to all employees. Recertification of entity level policies and procedures are performed on annual basics.

Disaster Preparedness

Every business is exposed to a range of threats, events and risks that could cause a disaster declaration. From power failures, fires, hazardous chemical spills, labor unrest, terrorist attacks on the company's facilities or nearby buildings, a disaster can quickly bring an organization's daily business operations to a halt. For this reason, Disaster Recovery (DR) and Business Continuity Planning (BCP) has become an essential element in LegalShield's strategic business plans.

DR and BCP provides LegalShield an increased level of confidence that its business processes and the IT data processing center are prepared to respond to disaster events and recover and resume daily business operations, while preparing to restore operations at a new or repaired business location.

During a declared disaster, senior management will authorize the relocation of Data Center services to an Alternate Site. LegalShield's recovery teams will implement the Alternate Site Recovery Strategy during an actual disaster to restore critical processing. LegalShield maintains, and annually tests, a comprehensive Business Continuity and Disaster Recovery Plan to mitigate the impact of disruptive conditions and major crises.

3 Description of Complementary User Entity Controls

The LegalShield system was designed with the assumption that internal controls would be placed in operation by user entities. The application of such internal controls by user entities is necessary to achieve certain criteria identified in this report. There may be additional criteria and related controls that would be appropriate for the security, availability, processing integrity, and confidentiality which are not identified in this report.

This section describes certain controls that user entities should consider for achievement of criteria identified in this report. The complementary user entity controls presented below should not be regarded as a comprehensive list of all the controls that should be employed by user entities:

Provisioning Accounts

- Customer management dictates to LegalShield the restricting authority of provisioning new member accounts within any LegalShield service.

Member Cancellation Procedures

- Members are responsible for contacting LegalShield in a timely manner to ensure cancelling accounts occurs prior to the next billing date.

General Controls

- Members are responsible for ensuring access to reports and other information generated from LegalShield is restricted.
- Users of LegalShield hosted applications are responsible for maintaining appropriate IT General Computer Controls and Application Controls.

Regulatory, Compliance, and Service Agreements

- Members are responsible for adhering to all regulatory compliance issues when they are associated with LegalShield in a service agreement.
- Members are responsible for reviewing and approving the terms and conditions stated in service agreements with LegalShield.

SECTION FOUR:

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

LegalShield designs its processes and procedures related to the systems used to meet its objectives for its Legal and Identity Theft monitoring and restoration services. Those objectives are based on the service commitments that LegalShield makes to its customers.

Security commitments to customers are documented and communicated in customer contracts, as well as in the description of the service offering provided. Security commitments include, but are not limited to, the following:

- Security principles within the fundamental designs of the LegalShield applications are designed to permit application users to access their information while restricting them from accessing the information of other users.
- Encryption technologies are used to protect customer data both at rest and while in transit.
- Firewalls and network segmentation are used to restrict traffic flow to only allow appropriate traffic.
- Logical access controls are in place as well as monitoring and regular reviews are done.
- Security monitoring of the infrastructure is in place including intrusion detection, centralized log management, and alerting.
- Data centers are geographically separated with multi-layered physical security in place.
- Vulnerability Management programs are designed to identify and correct vulnerabilities within the environment in a timely manner.
- Incident Response programs are designed to minimize the impact and protect resources.

LegalShield establishes operational requirements that support the achievement of our security commitments and other system requirements. Such requirements are communicated in LegalShield's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.